Self-Authentication of Electronic Evidence: New Rules 902(13)-(14)

Gregory P. Joseph*

Effective December 1, 2017, Rule 902 of the Federal Rules of Evidence was amended to add two provisions that authorize self-authentication of electronic evidence by certification.

Rule 902(13) allows use of a certification to authenticate evidence generated by an electronic process or system (*e.g.*, the contents of a website, data generated by an app, electronic entry/exit records of a security system). Rule 902(14) authorizes a certification to authenticate a digital copy of data taken from a device or system (*e.g.*, a mobile phone, a hard drive). This article focuses primarily on Rule 902(13) and its application in civil cases.

RULE 902(13)

Rule 902(13) provides that the following are self-authenticating:

> **(13)** ***Certified Records Generated by an Electronic Process or System.*** A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

Procedural Requirements. The certification under Rule 902(13) thus follows the procedural form of a 902(11) certification but dispenses with the business records foundation.[1] The procedural requirements of a Rule 902(13) certification drawn from 902(11) are: (i) the

---

* Past President, American College of Trial Lawyers (2010-11); Chair, ABA Section of Litigation (1997-98); member, Advisory Committee on the Federal Rules of Evidence (1993-99); Chair, Board of Trustees, Supreme Court Historical Society; author, SANCTIONS: THE FEDERAL LAW OF LITIGATION ABUSE (5th ed. 2013; Supp. 2018); CIVIL RICO: A DEFINITIVE GUIDE (5th ed. 2018); MODERN VISUAL EVIDENCE (1984; Supp. 2018); Editorial Board, MOORE'S FEDERAL PRACTICE (3d ed.) (since 1995); Joseph Hage Aaronson LLC, New York (www.jha.com).

[1] Fed. R. Evid. 902(11) provides that the following are self-authenticating:

> **(11) Certified Domestic Records of a Regularly Conducted Activity.** The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them.

If the certification addresses a business record generated in a foreign country, Rule 902(12) applies. If the 902(13) certification is made in a foreign country, then it would look to Rule 902(12), rather than 902(11).

certification must comply with a federal statute or Supreme Court rule (*e.g.*, 28 U.S.C. § 1746), and (ii) the proponent must give reasonable written notice of its intent to offer the evidence and furnish both the evidence and the certification to its opponent in advance of using it.

Non-Conclusory Certification. Substantively, the 902(13) certification must, in the words of the Advisory Committee Note, "contain[] information that would be sufficient to establish authenticity were that information provided by a witness at trial."

The certification must therefore set forth the qualifications of the certifier (to show that s/he is a "qualified person"), the substance of the testimony that the certifier would give if s/he were to testify at trial, and the process that s/he followed to generate the electronic evidence submitted with the certification. The certification should not be conclusory, just as the witness's testimony at trial would not be conclusory were testimony required.

Example. The contents of a website may generally be authenticated with testimony that a witness typed in the website address; that s/he logged on to the site and reviewed what was there; and that the proffered printout or other exhibit fairly and accurately reflects what the witness saw.[2] Under Rule 902(13), a certification setting forth these facts can substitute for testimony and shift the burden to the opponent to raise sufficient doubt that the issue should not be presented to finder of fact to make a final determination. Bear in mind that the certification is aimed at satisfying the Court under Rule 901(a) that the evidence is authentic. The Court makes only the initial decision under Rule 104(a) whether the proponent has offered sufficient proof that a reasonable juror could find in favor of authenticity.[3] If the Court so finds, then, under

---

[2] *See, e.g., O'Connor v. Newport Hospital*, 111 A.3d 317, 324 (R.I. 2015); *SEC v. Berrettini*, 2015 U.S. Dist. LEXIS 115963, at *21 (N.D. Ill. Sept 1, 2015).

[3] Fed. R. Evid. 104(a) provides: "The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege."

Rule 104(b),[4] the jury makes the final determination whether the evidence is, in fact, authentic.[5]

To make the certification more persuasive to the Court, it may be useful to point out other indicia of reliability in the certification. Continuing with the website evidence example, additional indicia of reliability that a certification might point out, depending on the experience and credentials of the witness, could include:

- Distinctive website design, logos, photos or other images associated with the website or its owner.
- That the contents of the webpage are of a type ordinarily posted on that website or websites of similar entities.
- That the contents of the webpage remain on the website for the court to verify.
- That the owner of the website has elsewhere published the same contents, in whole or in part.
- That the contents of the webpage have been republished elsewhere and attributed to the website.
- The length of time the contents were posted on the website.[6]

Authenticity, Not Admissibility. The Advisory Committee Note emphasizes that the Rule 902(13) certification establishes only authenticity, not admissibility. Hearsay, relevance, best evidence—all of the rules governing admissibility (evidentiary and, in criminal cases, constitutional) must otherwise be satisfied.

In some circumstances, admissibility may be addressable in the certification itself.

Combining 902(11) & (13) Certifications. One way of addressing admissibility in the certification is to combine a 902(11) and 902(13) certification—for example, in a certification of a qualified person who can establish that the contents of a website are maintained in the ordinary

---

[4] Fed. R. Evid. 104(b) provides: "When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later."

[5] *See, e.g.*, *United States v. Vayner*, 769 F.3d 125, 129-30 (2014); *United States v. Mebrtatu*, 543 F. App'x 137, 140-41 (3d Cir. 2013).

[6] Joseph, MODERN VISUAL EVIDENCE § 15.02[1][a] (Supp. 2018).

course of business and that the process utilized to generate the results shown on the website are authentic. This could prove useful in authenticating, for example, a page drawn from the Wayback Machine or the website of an organization (party or non-party).

Pretrial/Scheduling Orders. Pretrial/scheduling orders should address how far in advance of trial the Rule 902(13) certification and evidence must be made available to the opponent. If that is not spelled out in an order, err on the side of giving plenty of notice to the opposition. A challenge to authenticity may require expert evidence.

In Limine. It will usually make sense to make a 902(13) certification the subject of a motion in limine, if authenticity is disputed.

Alternate Authentication Permitted. The Advisory Committee Notes to Rule 902(13) and (14) both emphasize that certifications are not mandatory or preclusive. These provisions not preclude establishing authenticity through other means—another alternative to testimony, for example, may be judicial notice.[7]

Summary Judgment & Other Hearings. Even before 902(13), parties have submitted affidavits or declarations in connection with summary judgment, injunctive applications and other hearings to authenticate digital evidence. These are now governed by Rule 902(13). A procedural part of Rule 902(11) that is incorporated in 902(13) requires advance notice be given to the adversary "[b]efore the trial *or hearing*." On summary judgment and in most other contexts (TROs may be an exception), there is time built into the briefing schedule for an opponent to respond, and that time may be sufficient to satisfy the notice requirement for a 902(13)-(14) certification. If there is any doubt, provide additional notice. This is also a potential subject for a scheduling order.

---

[7] *Id.* at § 15.02[1][c]; Joseph, *Judicial Notice of Internet Evidence*, U.S. LAW WEEK, Vol. 82, No. 34 (Mar. 11, 2014).

RULE 902(14)

Generating electronic discovery often involves making digital copies of devices or hard drives. Rule 902(14) is aimed at digital copies, making the following self-authenticating:

> **(14)** ***Certified Data Copied from an Electronic Device, Storage Medium, or File.*** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Many of the points made above with respect to Rule 902(13) apply equally to 902(14).[8]

Hash Value. The substance of a 902(14) certification will be a product of technology. The Advisory Committee Note discusses a current means of authenticating a digital copy:

> Today [December 2017], data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value." A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file.... [I]dentical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.

Tools. The case law reflects that Cellebrite is law enforcement's tool of choice for digital copying and extraction of all data from a mobile device currently.[9] Case law also indicates that there are other tools that are more discriminating, such as Lantern, which can limit extraction to categories of information such as text messages, images or videos.[10] Experts, however, not cases, are the only reliable source of technical information.

---

[8] Specifically, the paragraphs labeled Non-Conclusory Certification; Authenticity, Not Admissibility; Pretrial/Scheduling Orders; In Limine; Alternate Authentication Permitted; and Summary Judgment & Other Hearings.

[9] *See, e.g., People v. Kelso*, 2017 Cal. App. Unpub. LEXIS 3521, 2017 WL 2242968 (Cal. Ct. App. May 22, 2017) ("As even the defense expert acknowledged, the Cellebrite device used to extract the texts from [the] cell phone was the 'industry standard tool.'"); *Spencer v. Lunada Bay Boys*, 2017 U.S. Dist. LEXIS 217424, *34 (C.D. Cal. Dec. 13, 2017) ("one of the leading software tools to extract and preserve mobile device data").

[10] *See, e.g., United States v. Morales*, 2017 CCA LEXIS 757 (U.S. Army Ct. Crim. App. Dec. 13, 2017).